PATENT ABSTRACTS OF JAPAN

(11)Publication number : **11-250571**
(43)Date of publication of application : **17.09.1999**

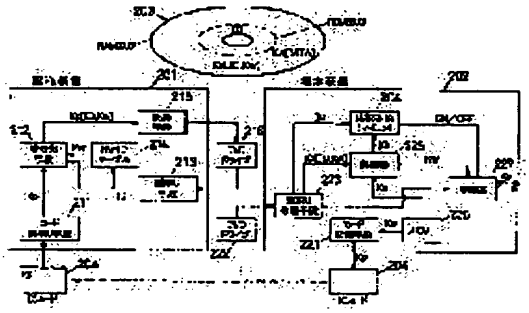
(51)Int.CI. **G11B 20/10**
G06F 12/14
G09C 1/00
H04L 9/32

(21)Application number : **10-052423**
(22)Date of filing : **04.03.1998**

(71)Applicant : **MATSUSHITA ELECTRIC IND CO LTD**
(72)Inventor : **TAKECHI HIDEAKI**
GOTO SHOICHI
IIZUKA HIROYUKI
YAMADA MASAZUMI

(54) INFORMATION DISTRIBUTING DEVICE, TERMINAL DEVICE AND INFORMATION DISTRIBUTING SYSTEM

(57)Abstract:
PROBLEM TO BE SOLVED: To provide an information distributing device, terminal device, and an information distributing system by which unauthorized copy to an other recording medium and use without permission can surely be prevented.
SOLUTION: A distributing device 201 is constituted with a card reading means 211 reading information of an IC card 204, a reading means 213 reading information of a DVD-RAM. a recording means 215 recording information in the DVD-RAM, a Kw ID table 214 converting an ID number to a cipher key Kw, and a ciphering means 212 ciphering information, and a terminal device 20 is constituted with a card recording means 221 recording information in the IC card 204, a memory 226 having a public key Kp and a secret key Ks, a reading and separating means 223 reading information of the DVD-RAM and separating it, decipherers 225, 227, deciphering ciphered information, and a comparing means 224 comparing two IDs.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平11－250571

(43)公開日　平成11年(1999)９月17日

(51)Int.Cl.[6]	識別記号	FI	
Ｇ１１Ｂ　20/10		Ｇ１１Ｂ　20/10	Ｈ
Ｇ０６Ｆ　12/14	３２０	Ｇ０６Ｆ　12/14	３２０Ｅ
Ｇ０９Ｃ　1/00	６３０	Ｇ０９Ｃ　1/00	６３０Ｆ
Ｈ０４Ｌ　9/32		Ｈ０４Ｌ　9/00	６７３Ｅ
			６７５Ａ

審査請求　未請求　請求項の数25　ＯＬ　（全 12 頁）

(21)出願番号　特願平10－52423

(22)出願日　平成10年(1998)３月４日

(71)出願人　000005821
松下電器産業株式会社
大阪府門真市大字門真1006番地

(72)発明者　武知　秀明
大阪府門真市大字門真1006番地　松下電器産業株式会社内

(72)発明者　後藤　昌一
大阪府門真市大字門真1006番地　松下電器産業株式会社内

(72)発明者　飯塚　裕之
大阪府門真市大字門真1006番地　松下電器産業株式会社内

(74)代理人　弁理士　松田　正道

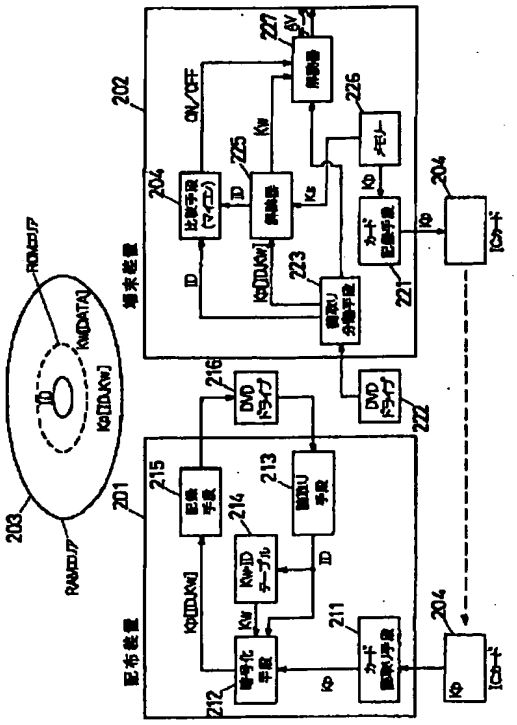
最終頁に続く

(54)【発明の名称】　情報配布装置と端末装置及び情報配布システム

(57)【要約】

【課題】　情報の配布に際し、鍵が盗まれたり、不正コピーが発生する恐れがあり、不正使用や無断使用を防止できない。

【解決手段】　配布装置２０１は、ＩＣカード２０４の情報を読み取るカード読取り手段２１１、ＤＶＤ－ＲＡＭの情報を読み取る読取り手段２１３、ＤＶＤ－ＲＡＭに情報を記録する記録手段２１５、ＩＤ番号を暗号鍵Ｋｗに変換するＫｗ・ＩＤテーブル２１４、情報を暗号化する暗号化手段２１２で構成され、端末装置２０２は、ＩＣカード２０４に情報を記録するカード記録手段２２１、公開鍵Ｋｐと秘密鍵Ｋｓを持つメモリ２２６、ＤＶＤ－ＲＡＭの情報を読み取り分離する読取り分離手段２２３、暗号化情報を解読する解読器２２５，２２７、２つのＩＤを比較する比較手段２２４により構成される。



【特許請求の範囲】

【請求項１】　記録媒体固有のＩＤ番号を持ち公開鍵Ｋｐが記録された情報記録媒体から、前記ＩＤ番号及び公開鍵Ｋｐを読み取る鍵読取り手段と、その読み取ったＩＤ番号及び所定の情報を前記読み取った公開鍵Ｋｐにより暗号化する暗号化手段と、その暗号化したＩＤ番号及び所定の情報を前記情報記録媒体に記録する記録手段とを備えたことを特徴とする情報配布装置。

【請求項２】　請求項１の前記情報配布装置で、前記公開鍵Ｋｐにより暗号化したＩＤ番号及び所定の情報が記録された前記情報記録媒体から、前記ＩＤ番号、暗号化ＩＤ番号及び、暗号化された所定の情報を読み取る暗号読取り手段と、前記公開鍵Ｋｐに対応する秘密鍵Ｋｓを用いて、前記読み取った暗号化ＩＤ番号及び所定の情報を復号する復号化手段と、その復号ＩＤ番号と前記ＩＤ番号とを比較するＩＤ比較手段と、その比較の結果、ＩＤ番号が一致した場合に、前記復号した所定の情報を適正であると判定する判定手段とを備えたことを特徴とする端末装置。

【請求項３】　請求項１の前記情報配布装置と、請求項２の前記端末装置とを備えたことを特徴とする情報配布システム。

【請求項４】　記録媒体固有のＩＤ番号を持つ情報記録媒体から、前記ＩＤ番号を読み取るＩＤ読取り手段と、公開鍵Ｋｐが記録された鍵記録媒体から前記公開鍵Ｋｐを読み取る鍵読取り手段と、その読み取った公開鍵Ｋｐにより前記読み取ったＩＤ番号及び所定の情報を暗号化する暗号化手段と、その暗号化したＩＤ番号及び所定の情報を前記情報記録媒体に記録する記録手段とを備えたことを特徴とする情報配布装置。

【請求項５】　請求項４の前記情報配布装置で、前記公開鍵Ｋｐにより暗号化したＩＤ番号及び所定の情報が記録された前記情報記録媒体から、前記ＩＤ番号、暗号化ＩＤ番号及び、暗号化された所定の情報を読み取る暗号読取り手段と、前記公開鍵Ｋｐに対応する秘密鍵Ｋｓを用いて、前記読み取った暗号化ＩＤ番号及び所定の情報を復号する鍵復号化手段と、その復号ＩＤ番号と前記ＩＤ番号とを比較するＩＤ比較手段と、その比較の結果、ＩＤ番号が一致した場合に、前記復号した所定の情報を適正であると判定する判定手段とを備えたことを特徴とする端末装置。

【請求項６】　請求項４の前記情報配布装置と、請求項５の前記端末装置とを備えたことを特徴とする情報配布システム。

【請求項７】　記録しようとするデータの識別情報が記録された情報記録媒体から前記識別情報を読み取る識別情報読取り手段と、その識別情報に基づいて所定の情報を生成する情報生成手段と、記録媒体固有のＩＤ番号及び公開鍵Ｋｐが記録された鍵記録媒体から、前記ＩＤ番号及び前記公開鍵Ｋｐを読み取る鍵読取り手段と、その読み取った公開鍵Ｋｐにより前記読み取ったＩＤ番号及び前記所定の情報を暗号化する暗号化手段と、その暗号化したＩＤ番号及び所定の情報と前記読み取った識別情報とを前記鍵記録媒体に記録する情報記録手段とを備えたことを特徴とする情報配布装置。

【請求項８】　請求項７の前記情報配布装置で、前記公開鍵Ｋｐにより暗号化したＩＤ番号及び所定の情報と前記識別情報とが記録された前記鍵記録媒体から、前記ＩＤ番号、暗号化ＩＤ番号、暗号化された所定の情報及び、識別情報を読み取る暗号読取り手段と、前記識別情報に対応する暗号化ＩＤ番号及び所定の情報を選択する選択手段と、前記公開鍵Ｋｐに対応する秘密鍵Ｋｓを用いて、前記選択した暗号化ＩＤ番号及び所定の情報を復号する復号化手段と、その復号ＩＤ番号と前記ＩＤ番号とを比較するＩＤ比較手段と、その比較の結果、ＩＤ番号が一致した場合に、前記識別情報に応じて、前記復号した所定の情報を適正であると判定する判定手段とを備えたことを特徴とする端末装置。

【請求項９】　請求項７の前記情報配布装置と、請求項８の前記端末装置とを備えたことを特徴とする情報配布システム。

【請求項１０】　記録媒体固有のＩＤ番号を持つ情報記録媒体から、前記ＩＤ番号を読み取るＩＤ読取り手段と、公開鍵Ｋｐが記録された鍵記録媒体から前記公開鍵Ｋｐを読み取る鍵読取り手段と、その読み取った公開鍵Ｋｐにより前記読み取ったＩＤ番号及び所定の情報を暗号化する鍵暗号化手段と、その暗号化したＩＤ番号及び所定の情報を前記鍵記録媒体とは別の鍵記録媒体に記録する鍵記録手段とを備えたことを特徴とする情報配布装置。

【請求項１１】　前記別の鍵記録媒体が、前記情報記録媒体の所定場所に設けられていることを特徴とする請求項１０に記載の情報配布装置。

【請求項１２】　請求項１０または１１の前記情報配布装置で、前記公開鍵Ｋｐにより暗号化したＩＤ番号及び所定の情報が記録された前記別の鍵記録媒体から、前記暗号化ＩＤ番号及び、暗号化された所定の情報を読み取る暗号読取り手段と、前記情報記録媒体からＩＤ番号を読み取るＩＤ読取り手段と、前記公開鍵Ｋｐに対応する秘密鍵Ｋｓを用いて、前記読み取った暗号化ＩＤ番号及び所定の情報を復号する復号化手段と、その復号ＩＤ番号と前記ＩＤ番号とを比較するＩＤ比較手段と、その比較の結果、ＩＤ番号が一致した場合に、前記復号した所定の情報を適正であると判定する判定手段とを備えたことを特徴とする端末装置。

【請求項１３】　請求項１０または１１の前記情報配布装置と、請求項１２の前記端末装置とを備えたことを特徴とする情報配布システム。

【請求項１４】　記録媒体固有のＩＤ番号を持つ情報記録媒体から前記ＩＤ番号を読み取るＩＤ読取り手段と、

公開鍵Ｋｐが記録された鍵記録媒体から前記公開鍵Ｋｐを読み取る鍵読取り手段と、前記読み取ったＩＤ番号に基づいて暗号鍵Ｋｗを生成する情報生成手段と、前記公開鍵Ｋｐにより前記ＩＤ番号及び前記暗号鍵Ｋｗを暗号化する暗号化手段と、その暗号化したＩＤ番号及び暗号鍵Ｋｗを前記情報記録媒体に記録する情報記録手段とを備え、前記情報記録媒体に記録されるデータは暗号鍵Ｋａにより暗号化され、前記暗号鍵Ｋａは前記暗号鍵Ｋｗで暗号化されて前記情報記録媒体に記録されていることを特徴とする情報配布装置。

【請求項１５】　請求項１４の前記情報配布装置で、前記公開鍵Ｋｐにより暗号化したＩＤ番号及び暗号鍵Ｋｗと前記暗号鍵Ｋｗにより暗号化した暗号鍵Ｋａとその暗号鍵Ｋａにより暗号化したデータとが記録された前記情報記録媒体から、前記ＩＤ番号、暗号化ＩＤ番号、暗号化暗号鍵Ｋｗ及び、暗号化暗号鍵Ｋａを読み取る暗号鍵読取り手段と、前記公開鍵Ｋｐに対応する秘密鍵Ｋｓを用いて、前記読み取った暗号化ＩＤ番号及び暗号化暗号鍵Ｋｗを復号する鍵復号化手段と、その復号した暗号鍵Ｋｗにより前記暗号鍵Ｋａを復号する暗号鍵復号手段と、前記復号ＩＤ番号と前記ＩＤ番号とを比較するＩＤ比較手段と、その比較の結果、ＩＤ番号が一致した場合に、前記復号した暗号鍵Ｋａにより前記情報記録媒体に記録された暗号化データを復号するデータ復号手段とを備えたことを特徴とする端末装置。

【請求項１６】　請求項１４の前記情報配布装置と、請求項１５の前記端末装置とを備えたことを特徴とする情報配布システム。

【請求項１７】　前記情報記録媒体に記録された暗号化データは、複数個に分割されたものであって、その分割されたデータ毎に前記暗号鍵Ｋａが異なることを特徴とする請求項１６記載の情報配布システム。

【請求項１８】　記録媒体固有の暗号鍵ＫＩＤを持つ情報記録媒体から、前記暗号鍵ＫＩＤを読み取る読取り手段と、公開鍵Ｋｐが記録された鍵記録媒体から前記公開鍵Ｋｐを読み取る鍵読取り手段と、前記読み取った暗号鍵ＫＩＤにより所定の情報を暗号化し、更にその暗号化した所定の情報を公開鍵Ｋｐにより暗号化する暗号化手段と、その暗号化した所定の情報を前記情報記録媒体に記録する記録手段とを備えたことを特徴とする情報配布装置。

【請求項１９】　請求項１８の前記情報配布装置で、前記暗号化した所定の情報が記録された前記情報記録媒体から、前記暗号鍵ＫＩＤ及び暗号化された所定の情報を読み取る暗号読取り手段と、前記公開鍵Ｋｐに対応する秘密鍵Ｋｓを用いて、前記読み取った暗号化された所定の情報を復号し、更にその復号した所定の情報を前記暗号鍵ＫＩＤにより復号する鍵復号化手段とを備えたことを特徴とする端末装置。

【請求項２０】　請求項１８の前記情報配布装置と、請求項１９の前記端末装置とを備えたことを特徴とする情報配布システム。

【請求項２１】　前記所定の情報が、金額情報または暗号鍵Ｋｗであることを特徴とする請求項３、６、９、１３、又は２０のいずれかに記載の情報配布システム。

【請求項２２】　所定の情報が金額情報であって、前記暗号化された金額情報を秘密鍵Ｋｓで復号して前記金額情報を得た後、前記暗号化された金額情報を消去し、その消去が成功した場合のみ、前記得た金額情報を有効と判定することを特徴とする請求項２１の情報配布システム。

【請求項２３】　所定の情報が金額情報であって、前記暗号化された金額情報を秘密鍵Ｋｓで復号して前記金額情報を得た後、その得た金額情報から使用分の金額を減額したときは、その減額後の金額情報を同一の暗号化方法により暗号化し、前記元の暗号化された金額情報を更新し、その更新が成功した場合のみ、前記減額を有効と判定することを特徴とする請求項２１の情報配布システム。

【請求項２４】　前記所定の情報は、少なくとも暗号鍵Ｋｗを含み、前記情報記録媒体には前記暗号鍵Ｋｗにより暗号化されたデータが記録されているものであって、前記判定手段により前記所定の情報が適正と判定された場合に、前記暗号鍵Ｋｗで暗号化されたデータを復号するデータ復号手段を備えたことを特徴とする請求項２、５、８、又は１２のいずれかに記載の端末装置。

【請求項２５】　前記暗号化されたデータは、複数のデータに分割されていることを特徴とする請求項２４記載の端末装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、暗号化された映画等のコンテンツを記録した記録媒体を配布し、ユーザがそれを購入して利用する情報配布装置及び端末装置と情報配布システムに関するものである。

【０００２】

【従来の技術】近年、映画や映像などの情報をＣＤ－ＲＯＭ、あるいはＤＶＤ－ＲＡＭなどの記録媒体に記録し、それをユーザに販売する方法が提案されている。このとき、情報の不正コピーによる使用や無断使用を防止するため、記録する情報を暗号化して、この暗号を解く鍵が無ければ映画や映像を見れないようにし、料金を支払った者のみこの暗号を解く鍵を入手して記録された情報を利用できるようにしている。従って、記録媒体に記録された暗号化情報は、不正コピーしたり、無断使用しようとしても、暗号を解く鍵を何らかの方法で入手しない限りは使用できない。

【０００３】

【発明が解決しようとする課題】しかしながら、このような方法では、暗号を解く鍵も暗号化情報が記録された

記録媒体と同様に、配布者側からユーザ側に伝達する必要があるため、盗まれたり、鍵そのものの不正コピーが発生する恐れがあり、その場合には、不正コピーによる使用や無断使用を防止できないという課題がある。

【０００４】本発明は、従来のこのような課題を考慮し、他の記録媒体への不正コピーや無断使用を確実に防止できる情報配布装置及び端末装置と情報配布システムを提供することを目的とするものである。

【０００５】

【課題を解決するための手段】請求項１の本発明は、記録媒体固有のＩＤ番号を持ち公開鍵Ｋｐが記録された情報記録媒体から、ＩＤ番号及び公開鍵Ｋｐを読み取る鍵読取り手段と、その読み取ったＩＤ番号及び所定の情報を読み取った公開鍵Ｋｐにより暗号化する暗号化手段と、その暗号化したＩＤ番号及び所定の情報を情報記録媒体に記録する記録手段とを備えた情報配布装置である。

【０００６】請求項２の本発明は、請求項１の情報配布装置で、公開鍵Ｋｐにより暗号化したＩＤ番号及び所定の情報が記録された情報記録媒体から、ＩＤ番号、暗号化ＩＤ番号及び、暗号化された所定の情報を読み取る暗号読取り手段と、公開鍵Ｋｐに対応する秘密鍵Ｋｓを用いて、読み取った暗号化ＩＤ番号及び所定の情報を復号する復号化手段と、その復号ＩＤ番号と前記ＩＤ番号とを比較するＩＤ比較手段と、その比較の結果、ＩＤ番号が一致した場合に、復号した所定の情報を適正であると判定する判定手段とを備えた端末装置である。

【０００７】請求項４の本発明は、記録媒体固有のＩＤ番号を持つ情報記録媒体から、ＩＤ番号を読み取るＩＤ読取り手段と、公開鍵Ｋｐが記録された鍵記録媒体から公開鍵Ｋｐを読み取る鍵読取り手段と、その読み取った公開鍵Ｋｐにより読み取ったＩＤ番号及び所定の情報を暗号化する暗号化手段と、その暗号化したＩＤ番号及び、所定の情報を情報記録媒体に記録する記録手段とを備えた情報配布装置である。

【０００８】請求項５の本発明は、請求項４の情報配布装置で、公開鍵Ｋｐにより暗号化したＩＤ番号及び所定の情報が記録された情報記録媒体から、ＩＤ番号、暗号化ＩＤ番号及び、暗号化された所定の情報を読み取る暗号読取り手段と、公開鍵Ｋｐに対応する秘密鍵Ｋｓを用いて、読み取った暗号化ＩＤ番号及び所定の情報を復号する鍵復号化手段と、その復号ＩＤ番号とＩＤ番号とを比較するＩＤ比較手段と、その比較の結果、ＩＤ番号が一致した場合に、復号した所定の情報を適正であると判定する判定手段とを備えた端末装置である。

【０００９】

【発明の実施の形態】以下に、本発明をその実施の形態を示す図面に基づいて説明する。

（第１の実施の形態）図１は、本発明にかかる第１の実施の形態の情報配布装置及び端末装置の機能を説明する構成図である。図１において、例えばＤＶＤ－ＲＡＭ１０３を記録媒体として用い、このＤＶＤ－ＲＡＭ１０３に映画などの情報（以後、配布情報と呼ぶ）を記録してユーザに配布する配布装置１０１と、ユーザが購入したＤＶＤ－ＲＡＭ１０３に記録された配布情報を再生する端末装置１０２により情報配布システムが構成されている。

【００１０】ここで、端末装置１０２は、公開鍵暗号方式の解読鍵となる秘密鍵Ｋｓが読み取り不可能な状態で内蔵され、ＤＶＤ－ＲＡＭ１０３には、記録媒体固有の一意に決まるＩＤ番号及び秘密鍵Ｋｓと対になる暗号化のための公開鍵Ｋｐが記録されている。ここでＫｓ及びＫｐは端末に固有である。また、配布情報は通常の暗号鍵Ｋｗにより暗号化され、予め記録されていてもよいし、配布時に記録するようにしてもよい。

【００１１】次に、上記実施の形態の情報配布装置及び端末装置の動作について、図面を参照しながら説明する。

【００１２】ユーザ配布情報を配布する場合、まず、配布装置１０１において、ＤＶＤ－ＲＡＭ１０３のＩＤ番号及び公開鍵Ｋｐを読み取り、公開鍵ＫｐによりＩＤ番号及び暗号鍵Ｋｗが暗号化される。この暗号化されたものを便宜上Ｋｐ［ＩＤ，Ｋｗ］で表す。ここでは、配布装置１０１が暗号鍵ＫｗとＩＤ番号との変換テーブルを持ち、暗号鍵Ｋｗは読み取ったＩＤ番号に基づいて生成されるものとする。配布情報が予め記録されている場合、変換テーブルはＩＤ番号から、予め記録された情報を暗号化した暗号鍵Ｋｗを特定するための変換作用を持つものとする。次に、暗号化されたＫｐ［ＩＤ，Ｋｗ］が、ＤＶＤ－ＲＡＭ１０３に記録される。配布情報を暗号鍵Ｋｗで暗号化したＫｗ［ＤＡＴＡ］もＤＶＤ－ＲＡＭ１０３に記録されている。

【００１３】次に、ユーザはこの状態のＤＶＤ－ＲＡＭ１０３を購入し、所有する端末装置１０２を用いてＤＶＤ－ＲＡＭ１０３を再生する。端末装置１０２において、まず、購入したＤＶＤ－ＲＡＭ１０３からＩＤ番号及びＫｐ［ＩＤ，Ｋｗ］を読み取り、その読み取ったＫｐ［ＩＤ，Ｋｗ］を内蔵する秘密鍵Ｋｓにより復号する。次に、復号したＩＤとＤＶＤ－ＲＡＭ１０３から直接読み取ったＩＤとを比較し、比較結果が一致した場合に、復号した暗号鍵Ｋｗを用いてＤＶＤ－ＲＡＭ１０３から読み取ったＫｗ［ＤＡＴＡ］を復号し、図示しないＡＶデコーダを通じて、ＴＶにより鑑賞する。

【００１４】この時、比較結果が一致しない場合は、ＩＤ番号が各記録媒体に固有であることから、情報が他のＤＶＤ－ＲＡＭにコピーされていると判断できるので、暗号鍵Ｋｗによる復号は停止される。

【００１５】また、Ｋｗによる配布情報の暗号化は共通鍵暗号方式により行うことが好適な構成である。これにより、復号に大きな計算量が必要な公開鍵の解読をＫｗ

を入手する際のみとし、映画などの大量の情報を容易に復号できる。

（第２の実施の形態）図２は、本発明にかかる第２の実施の形態の情報配布装置及び端末装置の機能を説明する構成図である。図２において、例えばＤＶＤ－ＲＡＭ２０３を情報記録媒体として用い、このＤＶＤ－ＲＡＭ２０３に映画などの情報（以後、配布情報と呼ぶ）を記録してユーザに配布する配布装置２０１と、ユーザが購入したＤＶＤ－ＲＡＭ２０３に記録された配布情報Ｋｗ［ＤＡＴＡ］を再生する端末装置２０２により情報配布システムが構成されている。本実施の形態では、前述の第１の実施の形態と異なり、公開鍵ＫｐをＤＶＤ－ＲＡＭ２０３ではなく、ユーザが端末装置２０２を用いて、例えばＩＣカード２０４等を用いた記録媒体（以後、鍵記録媒体と呼ぶ）に記録して配布装置２０１に提供する方法をとる。

【００１６】ここで、端末装置２０２は、公開鍵暗号方式の解読鍵となる秘密鍵Ｋｓが読み取り不可能な状態で内蔵され、ＤＶＤ－ＲＡＭ２０３には、記録媒体固有の一意に決まるＩＤ番号が記録されている。また、前述と同様、配布情報は通常の暗号鍵Ｋｗにより暗号化され、予め記録されていてもよいし、配布時に記録するようにしてもよい。

【００１７】図３は、本実施の形態の配布装置及び端末装置の内部を示すブロック図である。配布装置２０１は、ＩＣカード２０４に記録された情報を読み取る鍵読取り手段としてのカード読取り手段２１１、ＤＶＤドライブ２１６で駆動されるＤＶＤ－ＲＡＭ２０３から情報を読み取るＩＤ読取り手段としての読取り手段２１３、ＤＶＤ－ＲＡＭ２０３に情報を記録する記録手段２１５、ＩＤ番号を暗号鍵Ｋｗに変換するＫｗ・ＩＤテーブル２１４、情報を暗号化する暗号化手段２１２により構成されている。

【００１８】一方、端末装置２０２は、ＩＣカード２０４に情報を記録するカード記録手段２２１、公開鍵Ｋｐ及びそれと対になる秘密鍵Ｋｓを格納するメモリ２２６、ＤＶＤドライブ２２２で駆動されるＤＶＤ－ＲＡＭ２０３から情報を読み取り分離する読取り分離手段２２３、暗号化情報を解読する２つの解読器２２５，２２７、２つの情報を比較する比較手段（例えば、マイコンで構成される）２２４により構成されている。ここで、読取り分離手段２２３が暗号読取り手段を構成し、解読器２２５が鍵復号化手段を構成し、比較手段２２４がＩＤ比較手段及び判定手段を構成している。

【００１９】また、ＤＶＤ－ＲＡＭ２０３は、ＲＯＭエリアとＲＡＭエリアで構成されており、配布装置２０１で記録するＫｐ［ＩＤ，Ｋｗ］はＲＡＭエリアに記録される。また、暗号化された配布情報Ｋｗ［ＤＡＴＡ］はＲＯＭエリア、あるいはＲＡＭエリアのどちらに記録されていてもよいが、ＲＯＭエリアの場合は予め記録しておく。

【００２０】次に、上記実施の形態の情報配布装置及び端末装置の動作について、図面を参照しながら説明する。

【００２１】ユーザ配布情報を配布する場合、まず、端末装置２０２において、カード記録手段２２１がメモリ２２６から公開鍵Ｋｐを読み出し、ＩＣカード２０４に記録する。次に、配布装置２０１において、その公開鍵Ｋｐが記録されたＩＣカード２０４からカード読取り手段２１１が公開鍵Ｋｐを読み取り、また、ＤＶＤドライブ２１６にセットされたＤＶＤ－ＲＡＭ２０３から読取り手段２１３が、そのＤＶＤ－ＲＡＭ２０３のＩＤ番号を読み取る。

【００２２】カード読取り手段２１１により読み取られた公開鍵Ｋｐは暗号化手段２１２に送られ、読取り手段２１３で読み取られたＩＤ番号は、Ｋｗ・ＩＤテーブル２１４及び暗号化手段２１２に送られる。Ｋｗ・ＩＤテーブル２１４では、ＩＤ番号に基づいて配布情報を暗号化するための暗号鍵Ｋｗを生成し、生成した暗号鍵Ｋｗを暗号化手段２１２に送る。次に、暗号化手段２１２は、ＩＤ番号及び暗号鍵Ｋｗを公開鍵Ｋｐにより暗号化し、この暗号化したＫｐ［ＩＤ，Ｋｗ］を記録手段２１５に送る。記録手段２１５は、この暗号化されたＫｐ［ＩＤ，Ｋｗ］をＤＶＤドライブを介してＤＶＤ－ＲＡＭ２０３のＲＡＭエリアに記録する。この時、前述したように、配布情報を暗号鍵Ｋｗで暗号化したＫｗ［ＤＡＴＡ］もＤＶＤ－ＲＡＭ２０３に記録されている。

【００２３】次に、ユーザはこの状態のＤＶＤ－ＲＡＭ２０３を、所有する端末装置２０２を用いてＤＶＤ－ＲＡＭ２０３を再生する。端末装置２０２において、まず、読取り分離手段２２３は、ＤＶＤドライブ２２２を介して、購入したＤＶＤ－ＲＡＭ２０３からＩＤ番号及びＫｐ［ＩＤ，Ｋｗ］を読み取り、それら情報を分離する。このとき、Ｋｗ［ＤＡＴＡ］も読み取られて分離される。分離されたＩＤ番号は比較手段２２４に、Ｋｐ［ＩＤ，Ｋｗ］は解読器２２５に、Ｋｗ［ＤＡＴＡ］は解読器２２７に、それぞれ送られる。

【００２４】解読器２２５はメモリ２２６から公開鍵Ｋｐと対になる秘密鍵Ｋｓを読み出し、その秘密鍵Ｋｓにより暗号化情報Ｋｐ［ＩＤ，Ｋｗ］を解読してＩＤ番号を比較手段２２４に送り、暗号鍵Ｋｗを解読器２２７に送る。比較手段２２４では、読取り分離手段２２３からのＩＤ番号と解読器２２５で解読されたＩＤ番号とが比較され、比較結果に応じてＯＮ／ＯＦＦ信号を解読器２２７に送る。すなわち、２つのＩＤ番号が一致すればＯＮ信号を出力し、一致しなければＯＦＦ信号を出力する。

【００２５】解読器２２７は、ＯＮ信号のとき解読器２２５からの暗号鍵Ｋｗによって、暗号化配布情報Ｋｗ［ＤＡＴＡ］を解読して映画等のＡＶデータを出力す

る。ＡＶデータは図示しないＡＶデコーダを通じて、ＴＶにより鑑賞する。

【００２６】前述の第１の実施の形態の場合と同様に、ＩＤ番号の比較結果が一致しない場合は、ＩＤ番号が各記録媒体に固有であることから、情報が他のＤＶＤ－ＲＡＭにコピーされていると判断できるので、暗号鍵Ｋｗによる復号は停止される。

【００２７】このように、本発明によれば、ＤＶＤ－ＲＡＭのオリジナルとコピーとを判定することができる。この判定を逃れることを困難とするためには、ＩＤを市販の機器によってはコピーできない領域（例えばＲＯＭか１回のみ書き込み可能な領域など）に記録しておくことが好適である。

【００２８】ここで、第３者が上記で説明した端末（以下では適正な端末と呼ぶ）によらず、上記で説明した情報記録媒体のオリジナルではなくそのコピーにより情報を取得しようとした場合を説明する。

【００２９】例えばＤＶＤ－ＲＡＭの固有のＩＤごと全てコピーが可能な装置を用いた場合、このようにして作ったコピーを、保持するＫｓが異なる他の端末で再生しようとすると、ＩＤやＫｗを正しく復号化することができないため、情報を得ることができない。

【００３０】また一方、特定の端末のＫｓが不正に暴露されるなどにより、他の端末に同一のＫｓを与えることが可能となった場合でも、本発明のコピー判定機能が働いている限りコピーにより生成された情報配布媒体から情報を得ることはできない。

【００３１】以上のように、本発明の配布方法は、配布媒体のコピー防止とユーザ端末の特定機能を同時に備えているため、第３者が不正コピーや、無断で他の端末で利用することによって情報を不正取得することは著しく困難となり、不正に不特定多数の端末に情報のコピーを配布する行為を防止する効果がある。

（第３の実施の形態）図４は、本発明にかかる第３の実施の形態の情報配布装置及び端末装置を示すブロック図である。本実施の形態に用いるＤＶＤ－ＲＡＭは図５に示すような記録形態であり、配布情報が複数に分割され、その分割された部分情報がそれぞれ異なる暗号鍵Ｋ１～Ｋ４で暗号化され、更に、各暗号鍵Ｋ１～Ｋ４が暗号鍵Ｋｗにより暗号化されている。すなわち、二重に暗号化されている。また、記録されている配布情報に対応して、それぞれの識別情報としてのタイトル名が記録されている。

【００３２】図４において、図５のＤＶＤ－ＲＡＭ３０３を情報記録媒体として用い、このＤＶＤ－ＲＡＭ３０３に映画などの情報（以後、配布情報と呼ぶ）を記録してユーザに配布する配布装置３０１と、ユーザが購入したＤＶＤ－ＲＡＭ３０３に記録された配布情報を再生する端末装置３０２により情報配布システムが構成されている。本実施の形態では、鍵記録媒体としてのＩＣカード３０４に固有のＩＤ番号を利用し、公開鍵ＫｐをＩＣカード３０４に記録して配布装置３０１に提供し、暗号化情報をＩＣカード３０４に記録する方法をとる。このＩＣカード３０４は、ＩＤ番号が予め記録されているＲＯＭエリアと情報を記録可能なＲＡＭエリアとを持つ。

【００３３】配布装置３０１は、ＩＣカード３０４に記録された情報を読み取る鍵読取り手段としてのカード読取り手段３１１、ＤＶＤドライブ３１６で駆動されるＤＶＤ－ＲＡＭ３０３から情報（タイトル名）を読み取る識別情報読取り手段としての読取り手段３１３、ＩＣカード３０４に情報を記録する情報記録手段としてのカード記録手段３１５、タイトル名を暗号鍵Ｋｗに変換する情報生成手段としてのＫｗ・タイトルテーブル３１４、情報を暗号化する暗号化手段３１２により構成されている。

【００３４】一方、端末装置３０２は、ＩＣカード３０４に情報を記録するカード記録手段３２１、公開鍵Ｋｐ及びそれと対になる秘密鍵Ｋｓを格納するメモリ３２６、ＤＶＤドライブ３２２で駆動されるＤＶＤ－ＲＡＭ３０３から情報を読み取り分離する読取り分離手段３２３、暗号化情報を解読する３つの解読器３２５，３２７，３２８、２つの情報を比較するＩＤ比較手段としての比較手段（例えば、マイコンで構成される）３２４、ＩＣカード３０４の情報を読み取る暗号読取り手段としてのカード読取り手段３２９、タイトル名に基づいて配布情報を選択する選択手段３３０により構成されている。ここで、解読器３２５が復号化手段を構成している。

【００３５】次に、上記実施の形態の情報配布装置及び端末装置の動作について、図面を参照しながら説明する。

【００３６】ユーザが配布情報を購入する場合、まず、端末装置３０２において、カード記録手段３２１がメモリ３２６から公開鍵Ｋｐを読み出し、ＩＤ番号が記録されたＩＣカード３０４に記録する。次に、配布装置３０１において、その公開鍵Ｋｐが記録されたＩＣカード３０４からカード読取り手段３１１がＩＤ番号及び公開鍵Ｋｐを読み取り、また、ＤＶＤドライブ３１６にセットされたＤＶＤ－ＲＡＭ３０３から読取り手段３１３が、配布情報のタイトル名を読み取る。

【００３７】カード読取り手段３１１により読み取られたＩＤ番号及び公開鍵Ｋｐは暗号化手段３１２に送られ、読取り手段３１３で読み取られたタイトル名は、Ｋｗ・タイトル名テーブル３１４及びカード記録手段３１５に送られる。Ｋｗ・タイトル名テーブル３１４では、タイトル名に基づいて配布情報を暗号化するための暗号鍵Ｋｗを生成し、生成した暗号鍵Ｋｗを暗号化手段３１２に送る。次に、暗号化手段３１２は、ＩＤ番号及び暗号鍵Ｋｗを公開鍵Ｋｐにより暗号化し、この暗号化したＫｐ［ＩＤ，Ｋｗ］をカード記録手段３１５に送る。カ

ード記録手段３１５は、この暗号化されたＫｐ［ＩＤ，Ｋｗ］及び暗号化されていないタイトル名をＩＣカード３０４のＲＡＭエリアに記録する。この時、前述したように、配布情報は４分割されて、暗号鍵Ｋ１～Ｋ４によりそれぞれ暗号化されており、それら暗号鍵Ｋ１～Ｋ４も暗号鍵Ｋｗで暗号化されている。配布情報の分割数は４に限定されるものではなく、暗号鍵の個数も分割数に応じて用意すればよい。尚、図５では、暗号化した配布情報をＫ１［ＤＡＴＡ］～Ｋ４［ＤＡＴＡ］で表している。

【００３８】次に、ユーザはこの状態のＤＶＤ－ＲＡＭ３０３を購入し、所有する端末装置３０２により、ＩＣカードに記録された情報を利用してＤＶＤ－ＲＡＭ３０３を再生する。端末装置３０２において、まず、カード読取り手段３２９は、ＩＣカード３０４に記録されたＩＤ番号、暗号化情報Ｋｐ［ＩＤ，Ｋｗ］、タイトル名を読み取り、選択手段３３０に送る。

【００３９】一方、読取り分離手段３２３は、ＤＶＤドライブ３２２を介して、購入したＤＶＤ－ＲＡＭ３０３からタイトル名、Ｋｗ［Ｋ１］～Ｋｗ［Ｋ４］、Ｋ１［ＤＡＴＡ］～Ｋ４［ＤＡＴＡ］を読み取り、それら情報を分離する。分離されたタイトル名は選択手段３３０に、Ｋｗ［Ｋ１］～Ｋｗ［Ｋ４］は解読器３２８に、Ｋ１［ＤＡＴＡ］～Ｋ４［ＤＡＴＡ］は解読器３２７に、それぞれ送られる。選択手段３３０は、ＩＤ番号を比較手段３２４に送るとともに、読取り分離手段３２３からのタイトル名に応じて、そのタイトル名に対応する暗号化情報Ｋｐ［ＩＤ，Ｋｗ］を選択し、そのＫｐ［ＩＤ，Ｋｗ］を解読器３２５に送る。

【００４０】解読器３２５はメモリ３２６から公開鍵Ｋｐと対になる秘密鍵Ｋｓを読み出し、その秘密鍵Ｋｓにより暗号化情報Ｋｐ［ＩＤ，Ｋｗ］を解読してＩＤ番号を比較手段３２４に送り、暗号鍵Ｋｗを解読器３２８に送る。解読器３２８は暗号鍵Ｋｗを用いて暗号情報Ｋｗ［Ｋ１］～Ｋｗ［Ｋ４］を解読して暗号鍵Ｋ１～Ｋ４を解読器３２７に出力する。

【００４１】また、比較手段３２４は、選択手段３３０からのＩＤ番号と解読器３２５で解読されたＩＤ番号とを比較し、比較結果に応じてＯＮ／ＯＦＦ信号を解読器３２７に送る。すなわち、２つのＩＤ番号が一致すればＯＮ信号を出力し、一致しなければＯＦＦ信号を出力する。

【００４２】解読器３２７は、ＯＮ信号のとき解読器３２８からの暗号鍵Ｋ１～Ｋ４によって、暗号化配布情報Ｋ１［ＤＡＴＡ］～Ｋ４［ＤＡＴＡ］をそれぞれ解読してＡＶデータを出力する。ＡＶデータは図示しないＡＶデコーダを通じて、ＴＶにより鑑賞する。

【００４３】前述の第１の実施の形態の場合と同様に、ＩＤ番号の比較結果が一致しない場合は、暗号鍵Ｋｗによる復号は停止されるとともに、暗号鍵Ｋｗ、ＩＤ番号がＤＶＤ－ＲＡＭと別の記録媒体で運ばれるため、より安全性が増し、更に、配布情報を暗号化する暗号鍵を二重にしているので、不正コピー、無断利用に対して更に安全度が高くなる。

（第４の実施の形態）図６は、本発明にかかる第４の実施の形態の情報配布装置及び端末装置を示すブロック図である。本実施の形態に用いるＤＶＤ－ＲＡＭは図７に示すような記録形態であり、前述の図５と同様に、配布情報が複数に分割され、その分割された部分情報がそれぞれ異なる暗号鍵Ｋ１～Ｋ４で暗号化され、更に、各暗号鍵Ｋ１～Ｋ４が暗号鍵Ｋｗにより暗号化されている。図５の場合と異なる点は、タイトル名は記録せず、ＲＯＭエリアが設けられ、そのＲＯＭエリアにＤＶＤ－ＲＡＭに固有のＩＤ番号が記録されている点である。

【００４４】図６において、図７のＤＶＤ－ＲＡＭ４０３を情報記録媒体として用い、このＤＶＤ－ＲＡＭ４０３に映画などの情報（以後、配布情報と呼ぶ）を記録してユーザに配布する配布装置４０１と、ユーザが購入したＤＶＤ－ＲＡＭ４０３に記録された配布情報を再生する端末装置４０２により情報配布システムが構成されている。本実施の形態では、前述の第２の実施の形態と同様に、公開鍵Ｋｐをユーザが端末装置４０２を用いて、鍵記録媒体としてのＩＣカード４０４に記録して配布装置４０１に提供し、暗号化された情報をＤＶＤ－ＲＡＭ４０３に記録する方法をとる。

【００４５】配布装置４０１は、ＩＣカード４０４に記録された情報を読み取る鍵読取り手段としてのカード読取り手段４１１、ＤＶＤドライブ４１６で駆動されるＤＶＤ－ＲＡＭ４０３から情報を読み取るＩＤ読取り手段としての読取り手段４１３、ＤＶＤ－ＲＡＭ４０３に情報を記録する記録手段４１５、ＩＤ番号を暗号鍵Ｋｗに変換する情報生成手段としてのＫｗ・ＩＤテーブル４１４、情報を暗号化する暗号化手段４１２により構成されている。

【００４６】一方、端末装置４０２は、ＩＣカード４０４に情報を記録するカード記録手段４２１、公開鍵Ｋｐ及びそれと対になる秘密鍵Ｋｓを格納するメモリ４２６、ＤＶＤドライブ４２２で駆動されるＤＶＤ－ＲＡＭ４０３から情報を読み取り分離する暗号鍵読取り手段としての読取り分離手段４２３、暗号化情報を解読する３つの解読器４２５，４２７，４２８、２つの情報を比較するＩＤ比較手段としての比較手段（例えば、マイコンで構成される）４２４により構成されている。ここで、解読器４２５が鍵復号化手段を構成し、解読器４２８が暗号鍵復号手段を構成し、解読器４２７がデータ復号手段を構成している。

【００４７】次に、上記実施の形態の情報配布装置及び端末装置の動作について、図面を参照しながら説明する。

【００４８】ユーザが配布情報を購入する場合、まず、

端末装置４０２において、カード記録手段４２１がメモリ４２６から公開鍵Ｋｐを読み出し、ＩＣカード４０４に記録する。次に、配布装置４０１において、その公開鍵Ｋｐが記録されたＩＣカード４０４からカード読取り手段４１１が公開鍵Ｋｐを読み取り、また、ＤＶＤドライブ４１６にセットされたＤＶＤ－ＲＡＭ４０３から読取り手段４１３が、そのＤＶＤ－ＲＡＭ４０３のＩＤ番号を読み取る。

【００４９】カード読取り手段４１１により読み取られた公開鍵Ｋｐは暗号化手段４１２に送られ、読取り手段４１３で読み取られたＩＤ番号は、Ｋｗ・ＩＤテーブル４１４及び暗号化手段４１２に送られる。Ｋｗ・ＩＤテーブル４１４では、ＩＤ番号に基づいて配布情報を暗号化するための暗号鍵Ｋｗを生成し、生成した暗号鍵Ｋｗを暗号化手段４１２に送る。次に、暗号化手段４１２は、ＩＤ番号及び暗号鍵Ｋｗを公開鍵Ｋｐにより暗号化し、この暗号化したＫｐ［ＩＤ，Ｋｗ］を記録手段４１５に送る。記録手段４１５は、この暗号化されたＫｐ［ＩＤ，Ｋｗ］をＤＶＤドライブを介してＤＶＤ－ＲＡＭ４０３のＲＡＭエリアに記録する。この時、前述したように、配布情報は４分割されて、暗号鍵Ｋ１～Ｋ４によりそれぞれ暗号化されており、それら暗号鍵Ｋ１～Ｋ４も暗号鍵Ｋｗで暗号化されている。配布情報の分割数は４に限定されるものではなく、暗号鍵の個数も分割数に応じて用意すればよい。

【００５０】次に、ユーザはこの状態のＤＶＤ－ＲＡＭ４０３を購入し、所有する端末装置４０２を用いてＤＶＤ－ＲＡＭ４０３を再生する。端末装置４０２において、まず、読取り分離手段４２３は、ＤＶＤドライブ４２２を介して、購入したＤＶＤ－ＲＡＭ４０３からＩＤ番号、暗号情報Ｋｐ［ＩＤ，Ｋｗ］、Ｋｗ［Ｋ１］～Ｋｗ［Ｋ４］、Ｋ１［ＤＡＴＡ］～Ｋ４［ＤＡＴＡ］を読み取り、それら情報を分離する。分離されたＩＤ番号は比較手段４２４に、Ｋｐ［ＩＤ，Ｋｗ］は解読器４２５に、Ｋｗ［Ｋ１］～Ｋｗ［Ｋ４］は解読器４２８に、Ｋ１［ＤＡＴＡ］～Ｋ４［ＤＡＴＡ］は解読器４２７に、それぞれ送られる。

【００５１】解読器４２５はメモリ４２６から公開鍵Ｋｐと対になる秘密鍵Ｋｓを読み出し、その秘密鍵Ｋｓにより暗号化情報Ｋｐ［ＩＤ，Ｋｗ］を解読してＩＤ番号を比較手段４２４に送り、暗号鍵Ｋｗを解読器４２８に送る。解読器４２８は暗号鍵Ｋｗを用いて暗号情報Ｋｗ［Ｋ１］～Ｋｗ［Ｋ４］を解読して暗号鍵Ｋ１～Ｋ４を解読器４２７に出力する。

【００５２】また、比較手段４２４は、読取り分離手段４２３からのＩＤ番号と解読器４２５で解読されたＩＤ番号とを比較し、比較結果に応じてＯＮ／ＯＦＦ信号を解読器４２７に送る。すなわち、２つのＩＤ番号が一致すればＯＮ信号を出力し、一致しなければＯＦＦ信号を出力する。

【００５３】解読器４２７は、ＯＮ信号のとき解読器４２８からの暗号鍵Ｋ１～Ｋ４によって、暗号化配布情報Ｋ１［ＤＡＴＡ］～Ｋ４［ＤＡＴＡ］をそれぞれ解読してＡＶデータを出力する。ＡＶデータは図示しないＡＶデコーダを通じて、ＴＶにより鑑賞する。

【００５４】前述の第１の実施の形態の場合と同様に、ＩＤ番号の比較結果が一致しない場合は、暗号鍵Ｋｗによる復号は停止されるとともに、更に、配布情報を暗号化する暗号鍵を二重にしているので、不正コピー、無断利用に対して更に安全度が高くなる。

（第５の実施の形態）図８は、本発明にかかる第５の実施の形態における記録媒体上の記録状態を示す図である。本実施の形態は、基本的には例えば、第２の実施の形態などと同じであるが、公開鍵Ｋｐにより暗号化されたＩＤ番号及び暗号鍵Ｋｗである暗号化情報Ｋｐ［ＩＤ，Ｋｗ］を、元の鍵記録媒体であるＩＣカードや情報記録媒体であるＤＶＤ－ＲＡＭ５０３のＲＡＭエリアに記録する代わりに、別の鍵記録媒体、例えば図８に示すように、ＤＶＤ－ＲＡＭ５０３の所定領域に設けられた鍵媒体（例えば、バーコード形式などによるもの）に記録するものである。尚、この別の鍵記録媒体はＤＶＤ－ＲＡＭ５０３上に設けることは、特に限定されるものではない。

（第６の実施の形態）図９は、本発明にかかる第６の実施の形態における記録媒体上の記録状態を示す図である。本実施の形態は、例えば第２の実施の形態において、ＩＤ番号の代わりにＤＶＤ－ＲＡＭ（情報記録媒体）６０３に固有の一意的に決まっている暗号鍵ＫＩＤをＲＯＭエリアに持たせて、これを利用するものであり、配布情報を暗号化するための暗号鍵Ｋｗを暗号鍵ＫＩＤにより暗号化し、この暗号化したＫＩＤ［Ｋｗ］を更に公開鍵Ｋｐによって暗号化して、その暗号化情報Ｋｐ［ＫＩＤ［Ｋｗ］］をＲＡＭエリアに記録するものである。この方法によれば、暗号鍵ＫＩＤがＤＶＤ－ＲＡＭに固有であるため、別のＤＶＤ－ＲＡＭにコピーされても、読み取った暗号鍵ＫＩＤが異なるため、仮に公開鍵Ｋｐと対になる秘密鍵Ｋｓを盗まれても暗号鍵Ｋｗを復号出来ず、不正利用が防止できる。

【００５５】例えば、第１の実施の形態では、Ｋｓが暴露され、かつ端末のコピー判定機能が解除された場合、固有のＩＤごと情報記録媒体のコピーができなくとも、他の端末でコピーの再生が行える可能性が残った。しかし、記録媒体に固有の鍵ＫＩＤを使う方式においては、更に、ＫＩＤごと情報記録媒体のコピーが行われた場合にだけ不正に再生が可能であり、より安全性が高くなる。

【００５６】なお、上記実施の形態では、いずれも公開鍵Ｋｐにより暗号化する所定の情報として暗号鍵としたが、これに限らず、例えば支払った金額の料金情報（課金情報）などであってもよい。あるいは又、それら両者を含んでいてもよい。料金情報を用いれば、支払った金

額分の情報のみ復号することにより、１枚の情報記録媒体に多種類の情報を記録して販売しても、ユーザが利用できる情報や利用回数を制限できる。上記の料金情報を用いる場合は、例えば、端末装置において、暗号化された料金情報を読み取って復号した後、その暗号化された料金情報を消去する。この消去が成功した場合に限り、復号した料金情報を有効とする。このようにすれば、料金情報が何度も再利用されることがなく、不正使用が防止できる。また、金額分の一部だけ情報を利用したときは、料金情報を更新する必要がある。この場合は、元の料金情報から使用金額分を減額した後、同じ暗号化方法で暗号化し、その暗号化した料金情報を元の暗号化情報に上書きし、その上書きが成功した場合に限り料金情報を有効とする。

【００５７】また、上記第３の実施の形態では、識別情報としてタイトル名を用いたが、これに限らず、識別情報は記録するデータのコンテンツを識別できるものであればよく、例えば、タイトルＩＤなどでもよい。

【００５８】また、上記実施の形態では、いずれも情報記録媒体としてＤＶＤ－ＲＡＭを例に説明したが、これに限らず、例えば、ＣＤ－ＲＯＭやＣＤ－Ｒ等であってもよい。

【００５９】また、上記実施の形態では、いずれも鍵記録媒体としてＩＣカードを例に説明したが、これに限らず、例えば、磁気カード等であってもよい。

【００６０】

【発明の効果】以上述べたところから明らかなように本発明は、記録媒体固有のＩＤ番号及び所定の情報を公開鍵暗号方式により暗号化し、その暗号化したＩＤ番号を復号したＩＤ番号と記録媒体から読み取ったＩＤ番号とを比較することにより、所定の情報が適正かどうかを判定しているので、他の記録媒体への不正コピーや無断使用を確実に防止できるという長所を有する。

【図面の簡単な説明】

【図１】本発明にかかる第１の実施の形態の情報配布装置及び端末装置の機能を説明する構成図である。

【図２】本発明にかかる第２の実施の形態の情報配布装置及び端末装置の機能を説明する構成図である。

【図３】同第２の実施の形態の情報配布装置及び端末装置を示すブロック図である。

【図４】本発明にかかる第３の実施の形態の情報配布装置及び端末装置を示すブロック図である。

【図５】同第３の実施の形態における記録媒体上の記録状態を示す図である。

【図６】本発明にかかる第４の実施の形態の情報配布装置及び端末装置を示すブロック図である。

【図７】同第４の実施の形態における記録媒体上の記録状態を示す図である。

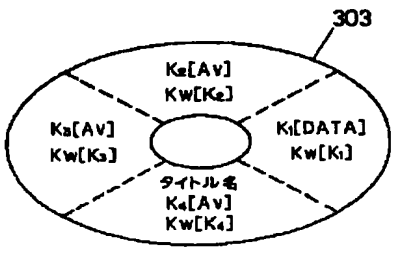
【図８】本発明にかかる第５の実施の形態における記録媒体上の記録状態を示す図である。

【図９】本発明にかかる第６の実施の形態における記録媒体上の記録状態を示す図である。

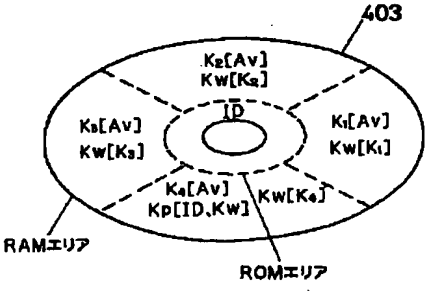
【符号の説明】

１０１、２０１、３０１、４０１　配布装置
１０２、２０２、３０２、４０２　端末装置
１０３、２０３、３０３、４０３、５０３、６０３　ＤＶＤ－ＲＡＭ
２０４、３０４、４０４　ＩＣカード
２１２、３１２、４１２　暗号化手段
２１５、４１５　記録手段
２２３、３２３、４２３　読取り分離手段
２２４、３２４、４２４　比較手段
２２５、３２５、４２５　解読器
２２７、３２７、４２７　解読器
３２８、４２８　解読器

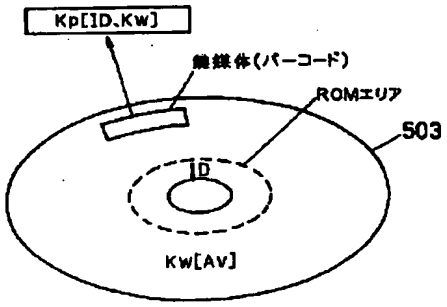
【図５】



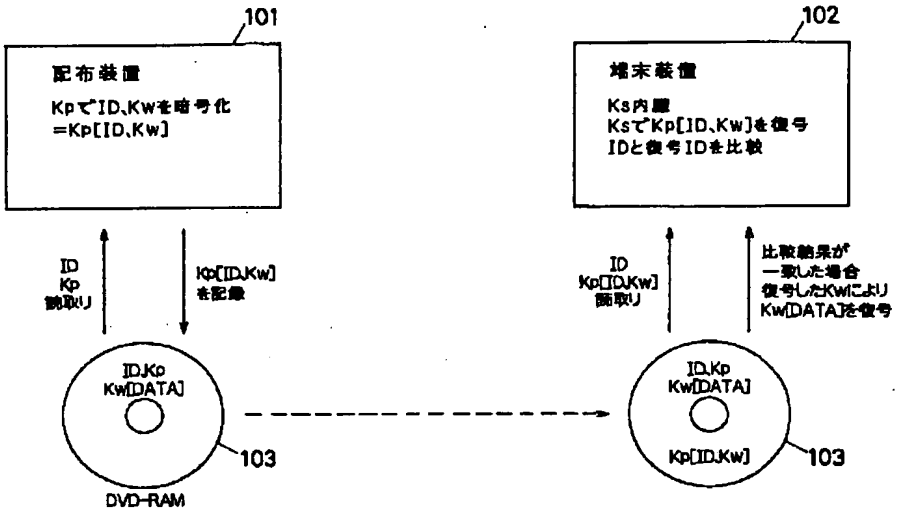
【図７】



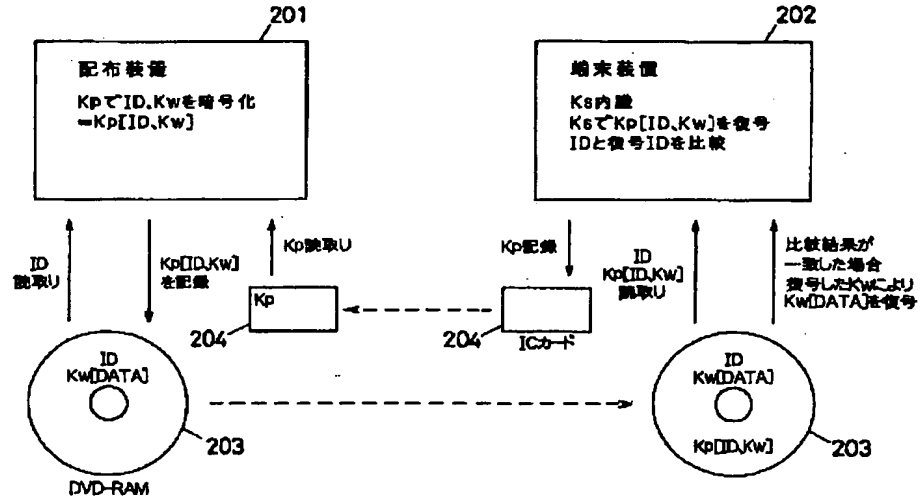
【図８】



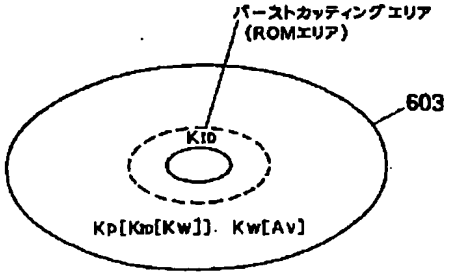
【図１】


101
配布装置
Kpで ID、Kwを暗号化
=Kp[ID、Kw]
102
端末装置
Ks内蔵
Ksで Kp[ID、Kw]を復号
IDと復号IDを比較
ID
Kp
読取り
Kp[ID,Kw]
を記録
ID
Kp[ID,Kw]
読取り
比較結果が
一致した場合
復号したKwにより
Kw[DATA]を復号
ID,Kp
Kw[DATA]
Kp[ID,Kw]
103
103
DVD-RAM

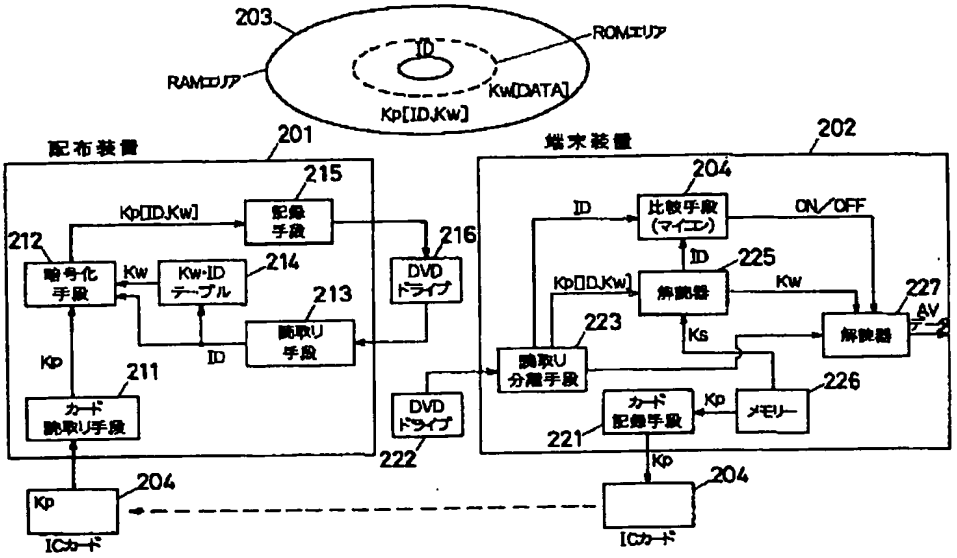
【図２】


201
配布装置
Kpで ID、Kwを暗号化
=Kp[ID、Kw]
202
端末装置
Ks内蔵
Ksで Kp[ID、Kw]を復号
IDと復号IDを比較
ID
読取り
Kp[ID,Kw]
を記録
Kp読取り
Kp記録
ID
Kp[ID,Kw]
読取り
比較結果が
一致した場合
復号したKwにより
Kw[DATA]を復号
Kp
204
204
ICカード
ID
Kw[DATA]
Kp[ID,Kw]
203
203
DVD-RAM

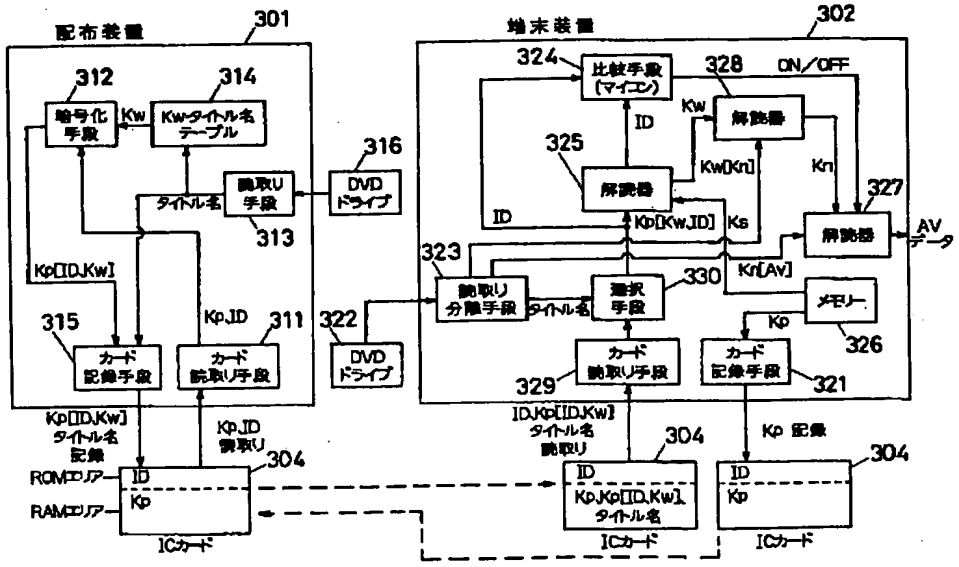
【図９】


バーストカッティングエリア
(ROMエリア)
603
KID
Kp[KID[Kw]]、Kw[Av]

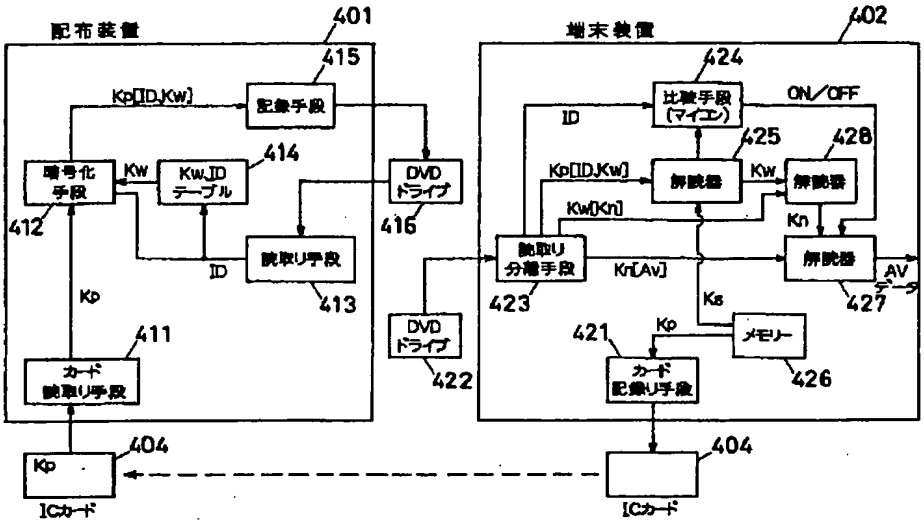
【図３】


203
ROMエリア
RAMエリア
ID
Kw[DATA]
Kp[ID,Kw]
配布装置
201
端末装置
202
215
記録手段
Kp[ID,Kw]
212
暗号化手段
Kw
Kw-ID テーブル
214
213
読取り手段
ID
Kp
211
カード読取り手段
DVDドライブ
216
222
204
ICカード
ID
比較手段(マイコン)
ON/OFF
225
解読器
Kw
227
AVデータ
223
読取り分離手段
Ks
226
メモリー
カード記録手段
221

【図４】


配布装置
301
端末装置
302
312
暗号化手段
Kw
314
Kw-タイトル名テーブル
316
DVDドライブ
読取り手段
タイトル名
313
Kp[ID,Kw]
315
カード記録手段
Kp,ID
311
カード読取り手段
322
DVDドライブ
Kp[ID,Kw] タイトル名 記録
Kp,ID 読取り
304
ROMエリア
RAMエリア
ID
Kp
ICカード
324
比較手段(マイコン)
328
ON/OFF
Kw
解読器
325
Kw[Kn]
Kn
327
AVデータ
Kp[Kw,ID]
Ks
323
読取り分離手段
タイトル名
330
選択手段
Kn[Av]
メモリー
Kp
326
カード読取り手段
329
カード記録手段
321
ID,Kp[ID,Kw] タイトル名 読取り
Kp 記録
Kp,Kp[ID,Kw] タイトル名

【図６】



フロントページの続き

(72)発明者　山田　正純
大阪府門真市大字門真1006番地　松下電器
産業株式会社内